THREATQUOTIENT™

Finanzdienstleistungsunternehmen nutzt ThreatQ™ zur Beschleunigung von Sicherheitsprozessen

Ein in den USA ansässiges globales Finanzdienstleistungsunternehmen ist Stolz darauf, dass es seinen Kunden bei der Steuerung von Risiken hilft, sodass sie ihr volles Potenzial besser nutzen können. Nun suchte das Unternehmen nach einer Möglichkeit, wie die volle Leistung der vorhandenen Ressourcen genutzt werden kann, um die eigenen Risiken besser zu steuern.

HERAUSFORDERUNG

Das Finanzdienstleistungsunternehmen abonniert zahlreiche Feeds mit globalen Bedrohungsdaten aus mehreren Quellen und erhält zudem fortlaufend eine immer größer werdende Menge an Protokoll- und Ereignisdaten von seinen internen Sicherheitssystemen und von SIEM. Das Vorhandensein unterschiedlicher Informationen an verschiedenen Orten war zu unübersichtlich geworden. Da die Tools nicht zusammengearbeitet haben, mussten die Analysten zwischen mehreren Portalen hin und her wechseln, um sich die Daten anzuschauen, alle scheinbar relevanten Daten manuell extrahieren, je nachdem, um welche Gruppe von Angreifern es gerade ging, und anschließend herausfinden, welche Schritte wie auszuführen sind.

Diese arbeitsintensive und taktische Vorgehensweise bei der Aktualisierung interner Sicherheitslösungen mit Indicators of Compromise (IoC) und kontextbezogenen Bedrohungsdaten wurde zudem dadurch erschwert, dass es zu wenig Personal für die Sicherheitsprozesse gab und die für Cyber Threat Intelligence (CTI) und Incident Response (IR) zuständigen Teams in getrennten Organisationen arbeiteten. „Ad-hoc-Analysen und -Maßnahmen waren zeitaufwendig, nicht zusammenhängend und ineffizient“, so der Sicherheitsingenieur des Unternehmens. „Wenn wir nicht gerade irgendwelche Brände löschten, reagierten wir auf den nächsten großen Angriff aus den Nachrichten und auf dringende Anrufe von der Unternehmensleitung.“

„Wir verfügen nun über IoC-Daten aus vertrauenswürdigen Quellen, die proaktiv in die Überwachungslisten zur Bedrohungserkennung bei verschiedenen internen Sicherheitslösungen integriert werden, wobei keine tägliche Überwachung durch die Teammitglieder benötigt wird. Darüber hinaus können wir ausgewählte Daten in das speziell für deren Nutzung ausgelegte Tool exportieren, sodass wir keine großen Datenmengen im Netzwerk übertragen müssen, was die Systeme verlangsamen würde.“

— Director of Threat Response

AUF EINEN BLICK

BRANCHE

Finanzdienstleistungen

HERAUSFORDERUNG

Das Vorhandensein unterschiedlicher Bedrohungsdaten an verschiedenen Orten sowie Ad-hoc-Analysen und -Maßnahmen seitens voneinander getrennter Teams waren zeitaufwendig, nicht zusammenhängend und ineffizient.

LÖSUNG

Die Threat Intelligence Platform ThreatQ sorgt dafür, dass die Teams und Technologien zusammenarbeiten können, um relevante Bedrohungen mit hoher Priorität zu erkennen und die Reaktionszeiten zu verkürzen, unter anderem durch die automatische Aktualisierung von Sicherheitskontrollen.

ERGEBNIS

- Proaktive Erkennung von und Reaktion auf Bedrohungen innerhalb von Stunden oder Tagen
- Effektivere Nutzung vorhandener Ressourcen ohne Umrüstung
- Ermittlung der geschäftlichen Auswirkungen und der Rendite von Sicherheitsprozessen

LÖSUNG

Das Unternehmen suchte nun nach einer Threat Intelligence Platform (TIP), um alle externen und internen Bedrohungs- und Ereignisdaten an einem Ort zu sammeln und somit die Risikobewertung und das Ergreifen von Maßnahmen zu erleichtern. Letztendlich benötigten sie eine Methode, bei der Bedrohungsinformationen für Sicherheitsprozesse über einen zentralen Kontrollpunkt genutzt werden können.

Das Team hatte folgende wesentlichen Anforderungen:

- Die Threat Intelligence Platform musste vor Ort sein, sodass sie die vollständige Kontrolle über ihre Daten und deren Sicherheit haben.
- Sie musste vorhandene und künftige Daten-Feeds unterstützen und individuelle Anpassungen ermöglichen. Bei seiner Suche fand das Evaluierungsteam heraus, dass einige Anbieter integrierte Daten-Feeds haben, die man nicht abschalten kann. Wenn sie also für die eigene Umgebung nicht relevant sind, entsteht dadurch nur mehr Datenmüll.
- Sie mussten die Möglichkeit haben, Unternehmenskontext automatisch auf eingehende externe Daten anzuwenden und die Daten im Hinblick auf dringende Probleme des Unternehmens nutzbar zu machen, um Maßnahmen priorisieren und zielgerichtet einsetzen zu können.
- Die Threat Intelligence Platform musste zudem eine zentrale Verwaltung und Kontrolle über die Verteilung von Daten auf interne Sicherheitslösungen bieten.

Das Unternehmen entschied sich für die Threat Intelligence Platform ThreatQ, nachdem sie festgestellt hatten, dass sie alle Anforderungen erfüllt. ThreatQ wird ständig mit globalen Bedrohungsdaten aus bestehenden Feeds des Unternehmens aktualisiert und durch interne kontextbezogene Bedrohungs-, Ereignis- und Vorfallsdaten ergänzt. Da Bedrohungsdaten basierend auf den vom Unternehmen festgelegten Parametern ausgewertet und gefiltert werden können, werden Bedrohungsinformationen fortlaufend priorisiert und neu priorisiert. Sämtliche Mitglieder des Sicherheitsteams, sogar die technisch nicht so versierten Mitarbeiter, können auf die für ihre Arbeit relevanten Bedrohungsinformationen zugreifen und weiterhin die Sicherheitstools nutzen, mit denen sie sich auskennen. ThreatQ unterstützt darüber hinaus die bidirektionale Integration, sodass Bedrohungs- und Ereignisdaten von SIEM, vom Ticket-System und von anderen Sicherheitstools in die Threat Intelligence Platform importiert werden können, damit die globalen Bedrohungsdaten kontextbezogen und relevant sind. Bedrohungsinformationen können auch im Rahmen bestehender Arbeitsabläufe und Prozesse in SIEM und diverse Sicherheitsebenen exportiert werden, um die Abwehr zu stärken.

„Wir verfügen nun über IoC-Daten aus vertrauenswürdigen Quellen, die proaktiv in die Überwachungslisten zur Bedrohungserkennung bei verschiedenen internen Sicherheitslösungen integriert werden, wobei keine tägliche Überwachung durch die Teammitglieder benötigt wird“, meint der Director of Threat Response des Unternehmens. „Darüber hinaus können wir ausgewählte Daten in das speziell für deren Nutzung ausgelegte Tool exportieren, sodass wir keine großen Datenmengen im Netzwerk übertragen müssen, was die Systeme verlangsamen würde.“

ERGEBNIS

Laut dem *Verizon Data Breach Investigations Report* 2017 nehmen die Mean-Time-To-Detect (MTTD) und Mean-Time-To-Respond (MTTR) weiterhin mehrere Monate in Anspruch. Mithilfe der ThreatQ-Plattform arbeiten die Sicherheitsteams des Finanzdienstleistungsunternehmens mit den Tools zusammen, um spezifische Zwischenfälle zu erkennen und innerhalb von Stunden oder Tagen entsprechende Maßnahmen zu ergreifen. „ThreatQ bietet mehr Transparenz hinsichtlich möglicher Vorgänge im Netzwerk oder in den Ressourcen des Unternehmens sowie die Integration vertrauenswürdiger IoC-Daten in interne Sicherheitslösungen nahezu in Echtzeit, sodass wir proaktiver und souverän handeln können“, meinte der Director of Threat Response.

ThreatQ erfüllt die Anforderungen des Sicherheitsteams im Hinblick auf Kontrolle und individuelle Anpassung, sodass sie die bereits vorhandenen Ressourcen besser nutzen können, um ihre Sicherheitsprozesse zu beschleunigen. Da sich die Plattform vor Ort befindet, können sie ihre Daten weiterhin eigenverantwortlich verwalten und den Datenaustausch kontrollieren. Und dank der Flexibilität und Offenheit der Plattform durch kundenspezifische Konnektoren ist sie problemlos für verschiedene Prozesse, Daten und Tools innerhalb des Unternehmens konfigurierbar, sodass keine Umrüstung erforderlich ist.

Das Team stellt fest, dass ThreatQ im Laufe der Zeit immer robuster wird. Die CTI- und IR-Teams nutzen dieses zentrale Repository, um ihre Daten zu speichern und weiterzuleiten, wodurch ihre Arbeit effizienter und effektiver wird. Da bei ThreatQ kundenspezifische Datenmodelle angewendet werden können und die Tools nicht mehr getrennt voneinander eingesetzt werden, ist eine Verfolgung mittels Indikatoren und die Ermittlung der geschäftlichen Auswirkungen möglich, sodass sich nachweislich eine höhere Rendite bei den Sicherheitsprozessen ergibt. Genau wie bei ihren eigenen Kunden können sie ihre Risiken besser steuern, um das volle Potenzial ihres Unternehmens zu nutzen.

ÜBER THREATQUOTIENT™

ThreatQuotient™ ist sich bewusst, dass Menschen die Grundlage für Intelligence-basierte Sicherheit darstellen. Die offene und erweiterbare Threat Intelligence Platform des Unternehmens, ThreatQ™, sowie die speziell für Krisenteams ausgelegte Lösung ThreatQ Investigations unterstützen Sicherheitsteams mit dem Kontext sowie den Möglichkeiten zur Anpassung und Priorisierung, die für fundiertere Entscheidungen, schnellere Erkennung und Reaktion sowie für die erweiterte Zusammenarbeit der Teams erforderlich sind. Führende weltweite Unternehmen verwenden ThreatQuotient-Lösungen als Grundpfeiler für ihre Sicherheitsabläufe und ihr Bedrohungsmanagementsystem.

Weitere Informationen finden Sie unter threatq.com.

TQ_ThreatQ-Financial-Services-Case-Study_Rev1